WHAT IS CLAIMED IS:

1. A method of providing security for a computer connected to a data store, the method comprising the steps of:

receiving an authentication key, a user name, and a computer identifier;

parsing the authentication key to obtain a parsed user name and computer identifier; and

validating the received user name and computer identifier using the parsed user name and computer identifier.

2. The method of claim 1, wherein validating comprises determining whether the received user name and computer identifier match the parsed user name and computer identifier.

3. The method of claim 2, wherein a match indicates that the received user name and computer identifier are valid.

4. The method of claim 1, further comprising, before parsing, decrypting the authentication key.

5. The method of claim 1, further comprising, if the received user name and computer identifier are valid, logging onto a server connected to the computer with a server user identifier and server password.

6. The method of claim 5, further comprising, parsing the authentication key to obtain the server user identifier and server password.

7. The method of claim 6, wherein multiple users share one server user identifier and server password.

8. The method of claim 1, further comprising generating the authentication key.

9. The method of claim 8, wherein the computer is connected to a client and a server and wherein the authentication key is generated with a client user name, a client computer identifier, a server user identifier, and a server password.

10. The method of claim 8, further comprising encrypting the authentication key.

11. The method of claim 8, further comprising forwarding the authentication key to a user.

12. The method of claim 1, wherein the computer is connected to a client and a server, and further comprising:

at the client, transmitting the authentication key, a client user name, and a client computer identifier to the server; and

at the computer,

intercepting the authentication key; and

if the user name and computer identifier are valid, logging onto the server.

13. An apparatus for providing security, comprising:

a computer having a data store connected thereto;

one or more computer programs, performed by the computer, for receiving an authentication key, a user name, and a computer identifier, parsing the authentication key to obtain a parsed user name and computer identifier, and validating the received user name and computer identifier using the parsed user name and computer identifier.

14. The apparatus of claim 13, wherein validating comprises determining whether the received user name and computer identifier match the parsed user name and computer identifier.

15. The apparatus of claim 14, wherein a match indicates that the received user name and computer identifier are valid.

16. The apparatus of claim 13, further comprising, before parsing, decrypting the authentication key.

17. The apparatus of claim 13, further comprising, if the received user name and computer identifier are valid, logging onto a server connected to the computer with a server user identifier and server password.

18. The apparatus of claim 17, further comprising, parsing the authentication key to obtain the server user identifier and server password.

19. The apparatus of claim 18, wherein multiple users share one server user identifier and server password.

20. The apparatus of claim 13, further comprising generating the authentication key.

21. The apparatus of claim 20, wherein the computer is connected to a client and a server and wherein the authentication key is generated with a client user name, a client computer identifier, a server user identifier, and a server password.

22. The apparatus of claim 20, further comprising encrypting the authentication key.

23. The apparatus of claim 20, further comprising forwarding the authentication key to a user.

24. The apparatus of claim 13, wherein the computer is connected to a client and a server, and further comprising:

at the client, transmitting the authentication key, a client user name, and a client computer identifier to the server; and

at the computer,

intercepting the authentication key; and

if the user name and computer identifier are valid, logging onto the server.

25. An article of manufacture comprising a computer program carrier readable by a computer and embodying one or more instructions executable by the computer to perform method steps for providing security to the computer connected to a data store, the method

receiving an authentication key, a user name, and a computer identifier;

parsing the authentication key to obtain a parsed user name and computer identifier; and

validating the received user name and computer identifier using the parsed user name and computer identifier.

26. The article of manufacture of claim 25, wherein validating comprises determining whether the received user name and computer identifier match the parsed user name and computer identifier.

27. The article of manufacture of claim 26, wherein a match indicates that the received user name and computer identifier are valid.

28. The article of manufacture of claim 25, further comprising, before parsing, decrypting the authentication key.

29. The article of manufacture of claim 25, further comprising, if the received user name and computer identifier are valid, logging onto a server connected to the computer with a server user identifier and server password.

30. The article of manufacture of claim 29, further comprising, parsing the authentication key to obtain the server user identifier and server password.

31. The article of manufacture of claim 30, wherein multiple users share one server user identifier and server password.

32. The article of manufacture of claim 25, further comprising generating the authentication key.

33. The article of manufacture of claim 32, wherein the computer is connected to a client and a server and wherein the authentication key is generated with a client user name, a client computer identifier, a server user identifier, and a server password.

34. The article of manufacture of claim 32, further comprising encrypting the authentication key.

35. The article of manufacture of claim 32, further comprising forwarding the authentication key to a user.

36. The article of manufacture of claim 25, wherein the computer is connected to a client and a server, and further comprising:

at the client, transmitting the authentication key, a client user name, and a client computer identifier to the server; and

at the computer,

intercepting the authentication key; and

if the user name and computer identifier are valid, logging onto the server.